Artículo original

Modelo para la evaluación en seguridad informática a productos software, basado en el estándar ISO/IEC 15408 Common Criteria

Evaluation model for computer security software products based on ISO/IEC 15408 Common Criteria

José Alejandro Chamorro, M.Sc.
Password Consulting Services, Cali (Colombia)
jose.chamorro@password.com.co

Francisco Pino, Ph.D.
Grupo de I&D en Ingeniería del Software
Universidad del Cauca (Colombia)
fjpino@ucauca.edu.co

Fecha de recepción: Noviembre 30 de 2011
Fecha de aceptación: Diciembre 21 de 2011

Palabras clave
Modela de evaluación, Common Criteria, cumplimiento, niveles, TOE, ST.

Keywords
Assessment model, Common Criteria, performance, levels, TOE, ST.

Colciencias tipo 1

Resumen

Las tecnologías de la información y las comunicaciones (TICs) presentan problemas en seguridad críticos, evidenciados con los múltiples fallos que son explotados por comunidades de crackers como Anonymous y generan grandes pérdidas en los sectores en que son implementadas en el mundo y en Colombia. El estándar ISO/IEC 15408 es uno de los más relevantes a nivel mundial en seguridad informática; a través del cumplimiento de siete niveles de evaluación (EAL1 – EAL7), garantiza seguridad en la operación controlada de una TIC. Desafortunadamente este estándar aun no está aplicado en el desarrollo de software en Colombia. Este artículo presenta un modelo que permite a los desarrolladores evaluar sus productos bajo el estándar ISO/IEC 15408 Common Criteria; en el, un software se conceptualiza en un Target of evaluation (TOE) y se evalúa de acuerdo a un Security Target (ST) oficial de Common Criteria en los dos primeros niveles (EAL1, *Probado Funcionalmente*, y EAL2, *Probado estructuralmente*) para identificar falencias en el cumplimiento y formular recomendaciones de mejora en seguridad, y acercarse así a procesos de certificación en Common Criteria.

Abstract

This article presents a model that enables software developers to evaluate their products under the ISO / IEC 15408 Common Criteria, starting with a risk analysis to several companies in Colombia, selected by the obligations to comply in the level of security law information, with an unfavorable outcome that demonstrate the need to implement the standard. From these results we developed a model, which achieves software conceptualized in a TOE (Target of evaluation) which corresponds to an ICT (Information and Communications), and evaluated according to a ST (Secure Target) Common Criteria portal officer, under the functions and required levels in order to identify shortcomings in compliance and safety recommendations for improvement.

1. Introducción

La complejidad de las medidas requeridas para el aseguramiento de los sistemas de información se hace mayor cada día, lo que obliga a todos los interesados a facilitar el desarrollo de esquemas que tengan en cuenta el carácter globalizado de las tecnologías de la Información, por la conectividad y disponibilidad necesaria y los problemas de delitos informáticos que son cada día más críticos. En los Estados Unidos, por ejemplo, se reportaron 303.909 incidentes de seguridad informática en el año (Internet Crime Complaint Center [IC³], 2010) y se determinaron pérdidas económicas de gastos directos del 57,6% de acuerdo al *Computer Crime and Security Survey* (Computer Security Institute [CSI], 2011).

Esto se suma a los problemas que puso en evidencia Anonymous, la comunidad de hackers más popular en la actualidad, el 30 de Noviembre de 2011, cuando aseguró haber accedido a cuentas de clientes importantes de Chase Bank y Bank of America y a tarjetas de crédito de Citibank, con el propósito de sacar dinero de ellas y dárselo a los pobres.

Figura 1. Amenaza de Anonymous contra los bancos (PoisAnon, 2011)

Portales como www.zone-h.org ponen al descubierto vulnerabilidades muy graves explotadas en sistemas informáticos de entidades públicas y privadas. Y los casos reportados incluyen empresas e instituciones colombianas. Y hay casos de seguridad informática que han tenido gran notoriedad en Colombia. El 19 de Febrero del 2010 un hacker con el alias de "syskc0" realizó un ataque de XSS (Cross Site Scripting) al sitio Web principal de UNE. A fines de noviembre de 2011 (zone-h.org). El Espectador

reportó un caso en la Alcaldía de Bogotá donde se manipularon las bases de datos del sistema de información que controla el proceso de impuestos, para disminuir el valor de las facturas de manera fraudulenta (Fraude en impuestos, 2011). Todo este panorama evidencia que las tecnologías de la información y las comunicaciones se ven afectadas por serios problemas en seguridad.

Figura 2. Ataque a UNE el 19 de febrero del 2010 (zona-h.org)

La seguridad en los componentes de las tecnologías de la información –Seguridad Informática– es una necesidad fundamental debido a que un fallo en ella genera un impacto directo en contra del objetivo por el cual fueron concebidos los componentes (Cano, 2004).

Para la seguridad de las tecnologías de la información existen varios siguientes estándares y buenas prácticas (Cano, Samudio, Prandini, Corozo, & Almanza, 2011):

ISO 27001 (Information Technology - Security techniques - Information security management systems - Requirements). Aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization (ISO) y la comisión International Electrotechnical Commission (IEC). Especifica los requisitos para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI). Es consistente con las mejores prácticas descritas en ISO/IEC 27002 y tiene su origen en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution, BSI (López & Ruiz, 2005a).

Cobit (Control Objectives for Information and related Technology). Conjunto de *Mejores Prácticas* para el manejo de información, creado por Information Systems Audit and Control Association (ISACA) y el IT Governance Institute (ITGI) en 1992 (ISACA, 2011).

Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas). Metodología de carácter público del Ministerio de Administraciones Públicas de España. Fue elaborado por el Consejo superior de administración pública (Dirección General para el Impulso de la Administración Electrónica, 2011).

Octave (Operationally Critical Threat, Asset, and Vulnerability Evaluation). Suite de herramientas técnicas y métodos que soportan una metodología de evaluación de riesgos desarrollada por el Software Engineering Institute (SEI) de la Carnegie Mellon University (SEI, 2008).

NIST Guidelines. Guías de referencia para la medición, el diseño y el desarrollo de tecnología del National Institute of Standards and Technology de los Estados Unidos (NIST, 2011).

Guías de la ENISA. Conjunto de guías generadas por la European Network of Information Security Agency, que busca establecer estándares y difundir Mejores Prácticas para el mejoramiento de las redes y la seguridad de la información en la Unión Europea (Enisa, 2011).

Top 20 de las fallas de seguridad. Presentación anual de los fallos de seguridad informática más críticas hecha por el *SysAdmin Audit, Networking and Security (SANS*) de los Estados Unidos (SANS, 2011).

OSSTMM (Open Standard Security Testing Model). Manual de la Metodología Abierta de *Testeo* de Seguridad desarrollado por ISECOM (Institute for Security and Open Methodologies), que brinda una referencia para realizar análisis de seguridad informática en diferentes niveles (Herzog, 2010).

ISM3 (Information Security Management Maturity Model). Estándar para la creación de sistemas de gestión de la seguridad de la información basados en ITIL, ISO27001 o Cobit, a través de metodologías de análisis de riesgo que tienen como objetivo garantizar la consecución de los objetivos del negocio (Aceituno, 2006).

ITIL (Information Technology Infrastructure Library). Conjunto de conceptos y prácticas para la gestión de servicios, el desarrollo y/o las operaciones relacionadas con las tecnologías de la información (APM Group, 2007).

ISO/IEC 15408 Common Criteria. Conjunto de estándares sobre seguridad de productos TIC (Tecnologías de la Información y las Comunicaciones) utilizados por diferentes países, que genera un resultado de evaluación que establece un nivel de confianza en el grado en el que el producto TIC satisface la funcionalidad de seguridad y ha superado las medidas de evaluación aplicadas (Common Criteria, 2000).

El estándar de Common Criteria, según Symantec (2011) representa el estándar de seguridad universal. Es obligatorio para el desarrollo de productos del Departamento de Defensa de los EE.UU. En contraste, en Colombia su aplicación es de apenas el 2,8% (Almanza, 2011) y no existen (como tampoco en otro país de América Latina) laboratorios para testeo y certificación (Common Criteria, s.f). Esto representa una

oportunidad para iniciativas que tengan como propósito acercar éste estándar de seguridad universal al software en Colombia y ayudar a generar mejorar las medidas de prevención.

En Colombia el 92% de las empresas desarrolladoras de software son pequeñas y el 7% medianas (Apuestas para crecer, 2008) y no cuentan con el personal ni los recursos económicos para garantizar el cumplimiento de los protocolos de pruebas de vulnerabilidad exigidos en el contexto internacional. Asimismo el desarrollo en investigación sobre seguridad informática es incipiente y el número de expertos en seguridad es bajo. Aunque existen diversas iniciativas orientadas a la capacitación de profesionales en esta área, tales como diplomados y especializaciones ofrecidos por algunas universidades, y el salón de Informática y las Jornadas de Seguridad que organiza la ACIS, no se ha logrado acercar los procesos de desarrollo del software al estándar ISO/IEC 15408 Common Criteria.

El objetivo general de la investigación que origina este artículo fue formular y diseñar un modelo que permita implementar la evaluación en seguridad informática al software bajo el estándar ISO/IEC 15408 Common Criteria. Para cumplir con su cometido debió determinar un conjunto de productos software a los que se les puede aplicar la evaluación en seguridad informática basadas en la ISO/IEC 15408 Common Criteria, realizar un análisis de riesgo en seguridad informática siguiendo Common Criteria a los productos software establecidos, diseñar el modelo para la evaluación en seguridad informática de productos software de acuerdo a la ISO/IEC 15408 Common Criteria y evaluar el modelo en un producto software específico.

2. Método

2.1 Análisis de riesgo EAL en seguridad informática

Los criterios de evaluación para el análisis de riesgo del modelo utilizado se basan en los dos niveles de seguridad del ISO/IEC 15408-3 Common Criteria: EAL1, *Probado Funcionalmente*, y EAL2, *Probado estructuralmente*, en su controles agremiados en las clases: Administración de la Configuración, Entrega y Funcionamiento, Desarrollo, Documentos Guía, Pruebas, y Evaluación de la Vulnerabilidad.

A cada componente se le formula una pregunta que indaga sobre el cumplimiento de los requisitos del TOE bajo evaluación. Las respuestas sirven de base para *medir* un nivel de riesgo en seguridad asociado a dicho TOE. La información de la Tabla 1 hasta la Tabla 6 corresponde a las preguntas identificadas para cada componente.

EAL	Pregunta (componente)
EAL1	El desarrollador presentó una referencia para el TOE (ACM_CAP.1.1D)
	La referencia para el TOE es única para cada versión (ACM_CAP.1.1C)
	El TOE es etiquetado con su referencia (ACM_CAP.1.2C)
	El evaluador confirma que la información suministrada reúne todos los requerimientos para contenido y presentación de evidencia (ACM_CAP.1.1E)
EAL2	El desarrollador provee una referencia para el TOE (ACM_CAP.2.1D)
	El desarrollador usa un sistema de administración de configuración (ACM_CAP.2.2D)
	El desarrollador provee documentación del administrador de configuración (ACM_CAP.2.3D)
	La referencia para el TOE es única para cada versión (ACM_CAP.2.1C)
	El TOE es etiquetado con su referencia (ACM_CAP.2.2C)
	La documentación del administrador de configuración incluye una lista de configuración (ACM_CAP.2.3C)
	La lista de configuración identifica únicamente todos los ítems de configuración que abarca el TOE (ACM_CAP.2.4C)
	La lista de configuración describe los ítems de configuración que abarca el TOE (ACM_CAP.2.5C)
	La documentación del administrador de configuración describe el método utilizado para identificar únicamente los ítems de configuración (ACM_CAP.2.6C)
	El sistema de administrador de configuración identifica únicamente todos los ítems de configuración (ACM_CAP.2.7C)
	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia (ACM_CAP.2.1E)

Tabla 1. Clase: Administración de la Configuración - Preguntas para EAL1 y EAL2

EAL	Pregunta
EAL1	El desarrollador documenta los procedimientos necesarios para la instalación segura, generación y puesta en marcha del TOE (ADO_IGS.1.1D)
	La documentación indica los pasos necesarios para garantizar la instalación, generación y puesta en marcha del TOE (ADO_IGS.1.1C)
	El evaluador confirma que la información proporcionada cumple con todos los requisitos de contenido y la presentación de pruebas (ADO_IGS.1.1E)
	El evaluador determina que los procedimientos de instalación, generación y puesta en marcha son resultado de una configuración segura (ADO_IGS.1.2E)
EAL2	El desarrollador documenta los procedimientos de entrega del TOE ó partes de este al usuario (ADO_DEL.1.1D)
	El desarrollador utiliza los procedimientos de entrega (ADO_DEL.1.2D)
	La documentación entregada describe todos los procedimientos necesarios para mantener la seguridad cuando se distribuyen versiones del TOE a los usuarios (ADO_DEL.1.1C)
	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia (ADO_DEL.1.1E)
	El desarrollador provee una referencia para el TOE (ADO_IGS.1.1D)
	La referencia para el TOE es única para cada versión (ADO_IGS.1.1C)
	El TOE es etiquetado con su referencia (ADO_IGS.1.1E)
	El evaluador determina que los procedimientos de instalación, generación y puesta en marcha son resultado de una configuración segura (ADO_IGS.1.2E)

Tabla 2. Clase: Entrega y funcionamiento - Preguntas para EAL1 y EAL2

EAL	Pregunta
EAL1	El desarrollador provee una especificación funcional (ADV_FSP.1.1D)
	La especificación funcional describe el TSF y sus interfaces externas usando un lenguaje informal (ADV_FSP.1.1C)
	La especificación funcional es consistente internamente (ADV_FSP.1.2C)
	La especificación funcional describe el propósito y método de uso de todas las interfaces externas TSF, proveer detalles de los efectos, excepciones y mensajes de error (ADV_FSP.1.3C)
	La especificación funcional representa completamente la TSF (ADV_FSP.1.4C)

Tabla 3. Clase Desarrollo - Preguntas para EAL1 y EAL2

EAL	Pregunta
EAL2	La especificación funcional representa completamente la TSF (ADV_FSP.1.4C)
	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia (ADV_FSP.1.1E)
	El evaluador determina que la especificación funcional sea una exacta y completa instanciación de los requisitos funcionales de seguridad del TOE (ADV_FSP.1.2E)
	El desarrollador presenta un análisis de la correspondencia entre todos los pares adyacentes de representaciones de TSF que se ofrece (ADV_RCR.1.1D)
	Para cada par adyacente de representaciones TSF entregadas, el análisis demuestra que toda la funcionalidad de seguridad relevante de la representación TSF más abstracta está correctamente y completamente refinada en la representación TSF menos abstracta (ADV_RCR.1.1C)
	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia (ADV_RCR.1.1E)
EAL2	El desarrollador provee una especificación funcional (ADV_FSP.1.1D)
	La especificación funcional describe el TSF y sus interfaces externas usando un estilo informal (ADV_FSP.1.1C).
	La especificación funcional es internamente consistente (ADV_FSP.1.2C)
	La especificación funcional describe el objetivo y el método de uso de todas las interfaces externas de TSF, se facilitan detalles de los efectos, las excepciones y mensajes de error (ADV_FSP.1.3C)
	La especificación funcional representa completamente la TSF (ADV_FSP.1.4C)
	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia (ADV_FSP.1.1E)
	El evaluador determina que la especificación funcional sea una exacta y completa instanciación de los requisitos funcionales de seguridad del TOE (ADV_FSP.1.2E)
	El desarrollador presenta un análisis de la correspondencia entre todos los pares adyacentes de representaciones de TSF que se ofrece (ADV_RCR.1.1D)
	Para cada par adyacente de representaciones TSF entregadas, el análisis demuestra que toda la funcionalidad de seguridad relevante de la representación TSF más abstracta está correctamente y completamente refinada en la representación TSF menos abstracta (ADV_RCR.1.1C)
	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia (ADV_RCR.1.1E)
	El desarrollador entrega el diseño de alto nivel de la TSF (ADV_HLD.1.1D)
	La presentación del diseño de alto nivel es informal (ADV_HLD.1.1C)
	El diseño de alto nivel es internamente consistente (ADV_HLD.1.2C)

Tabla 3. Clase Desarrollo - Preguntas para EAL1 y EAL2 (cont.)

EAL	Pregunta
EAL2	El diseño de alto nivel describe la estructura de la TSF en términos de subsistemas (ADV_HLD.1.3C)
	El diseño de alto nivel describe la funcionalidad de seguridad suministrada por cada subsistema de la TSF (ADV_HLD.1.4C)
	El diseño de alto nivel debe identificar cualquier tipo de software requerido por la TSF, con una presentación de las funciones que ofrece el soporte a los mecanismos de protección aplicados en ese software (ADV_HLD.1.5C)
	El diseño de alto nivel identifica todas las interfaces para los subsistemas de la TSF (ADV_HLD.1.6C)
	El diseño de alto nivel identifica cuál de las interfaces para los subsistemas de las TSF son visibles externamente (ADV_HLD.1.7C)
	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia (ADV_HLD.1.1E)
	El evaluador determina que el diseño de alto nivel sea una exacta y completa instanciación de los requisitos funcionales de seguridad del TOE (ADV_HLD.1.2E)

Tabla 3. Clase Desarrollo - Preguntas para EAL1 y EAL2 (cont.)

EAL	Pregunta
EAL1	El desarrollador proporciona la guía del administrador dirigida al personal administrativo del sistema (AGD_ADM.1.1D)
	La guía del administrador describe las funciones administrativas e interfaces disponibles para el administrador del TOE (AGD_ADM.1.1C)
	La guía del administrador describe cómo administrar el TOE de una manera segura (AGD_ADM.1.2C)
	La guía del administrador contiene advertencias acerca de las funciones y privilegios que deben ser controlados en un ambiente seguro de procesamiento (AGD_ADM.1.3C)
	La guía del administrador describe todas las hipótesis respecto al comportamiento del usuario que son relevantes para el funcionamiento seguro del TOE (AGD_ADM.1.4C)
	La guía del administrador describe todos los parámetros de seguridad bajo el control del administrador, indicando los valores de seguridad apropiados (AGD_ADM.1.5C)

Tabla 4. Clase Documentos Guía - Preguntas para EAL1 y EAL2

EAL	Pregunta
EAL1	La guía administrador describe cada tipo de evento de seguridad pertinentes en relación con las funciones administrativas que deben ser realizadas, incluyendo el cambio de características de seguridad de las entidades bajo el control de la TSF (AGD_ADM.1.6C)
	La guía del administrador es consistente con toda la demás documentación suministrada para evaluación (AGD_ADM.1.7C)
	La guía del administrador describe todos los requerimientos de seguridad para el ambiente de tecnología de la información (AGD_ADM.1.8C)
	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia (AGD_ADM.1.1E)
	La guía del administrador describe las funciones administrativas e interfaces disponibles para el administrador del TOE (AGD_USR.1.1D)
	La guía del administrador describe cómo administrar el TOE de forma segura (AGD_USR.1.1C)
	La guía del administrador contiene advertencias acerca de funciones y privilegios que deben ser controladas en un ambiente de procesamiento seguro (AGD_USR.1.2C)
	La guía del administrador describe todas las hipótesis respecto al comportamiento del usuario que son relevantes para el funcionamiento seguro del TOE (AGD_USR.1.3C)
	La guía del administrador describe todos los parámetros bajo el control del administrador indicando los valores seguros apropiados (AGD_USR.1.4C)
	La guía administrador describe cada tipo de evento de seguridad pertinentes en relación con las funciones administrativas que deben ser realizadas, incluyendo el cambio de características de seguridad de las entidades bajo el control de la TSF (AGD_USR.1.5C)
	La guía del administrador es consistente con toda la demás documentación suministrada para evaluación (AGD_USR.1.6C)
	La guía del administrador describe todos los requerimientos de seguridad para el ambiente de tecnología de la información que son relevantes al administrador (AGD_USR.1.1E)
EAL2	El desarrollador proporciona la guía del administrador dirigida al personal administrativo del sistema (AGD_ADM.1.1D)
	La guía del administrador describe las funciones administrativas e interfaces disponibles para el administrador del TOE (AGD_ADM.1.1C)
	La guía del administrador describe cómo administrar el TOE de forma segura (AGD_ADM.1.2C)

Tabla 4. Clase Documentos Guía - Preguntas para EAL1 y EAL2 (cont.)

EAL	Pregunta
	La guía del administrador contiene advertencias acerca de las funciones y privilegios que deben ser controlados en un ambiente seguro de procesamiento (AGD_ADM.1.3C)
	La guía del administrador describe todas las hipótesis respecto al comportamiento del usuario que son relevantes para el funcionamiento seguro del TOE (AGD_ ADM.1.4C)
	La guía del administrador describe todos los parámetros de seguridad bajo el control del administrador, indicando los valores de seguridad apropiados (AGD_ADM.1.5C)
	La guía administrador describe cada tipo de evento de seguridad pertinentes en relación con las funciones administrativas que deben ser realizadas, incluyendo el cambio de características de seguridad de las entidades bajo el control de la TSF (AGD_ADM.1.6C)
	La guía del administrador es consistente con toda la demás documentación suministrada para evaluación (AGD_ADM.1.7C)
	La guía del administrador describe todos los requerimientos de seguridad para el ambiente de tecnología de la información (AGD_ADM.1.8C)
	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia (AGD_ADM.1.1E)
EAL2	La guía del administrador describe las funciones administrativas e interfaces disponibles para el administrador del TOE (AGD_USR.1.1D)
	La guía del administrador describe cómo administrar el TOE de forma segura (AGD_USR.1.1C)
	La guía del administrador contiene advertencias acerca de funciones y privilegios que deben ser controladas en un ambiente de procesamiento seguro (AGD_USR.1.2C)
	La guía del administrador describe todas las hipótesis respecto al comportamiento del usuario que son relevantes para el funcionamiento seguro del TOE (AGD_ USR.1.3C)
	La guía del administrador describe todos los parámetros bajo el control del administrador indicando los valores seguros apropiados (AGD_USR.1.4C)
	La guía administrador describe cada tipo de evento de seguridad pertinentes en relación con las funciones administrativas que deben ser realizadas, incluyendo el cambio de características de seguridad de las entidades bajo el control de la TSF (AGD_USR.1.5C)
	La guía del administrador es consistente con toda la demás documentación suministrada para evaluación (AGD_USR.1.6C)
	La guía del administrador describe todos los requerimientos de seguridad para el ambiente de tecnología de la información que son relevantes al administrador (AGD_USR.1.1E)

Tabla 4. Clase Documentos Guía - Preguntas para EAL1 y EAL2 (cont.)

EAL	Pregunta
EAL1	El desarrollador provee el TOE para pruebas (ATE_IND.1.1D)
	El TOE se adecua para pruebas (ATE_IND.1.1C)
	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia (ATE_IND.1.1E)
	El evaluador prueba un subconjunto de la TSF apropiadamente para confirmar que el TOE funciona como se especificó (ATE_IND.1.2E)
EAL2	El desarrollador provee evidencia del cubrimiento de la prueba (ATE_COV.1.1D)
	La evidencia del cubrimiento de la prueba muestra la correspondencia entre las pruebas identificadas en la documentación de pruebas y la TSF descrita en la especificación funcional (ATE_COV.1.1C)
	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia (ATE_COV.1.1E)
	El desarrollador prueba el TSF y documenta los resultados (ATE_FUN.1.1D)
	El desarrollador provee la documentación de pruebas (ATE_FUN.1.2D)
	La documentación de pruebas consiste en planes de pruebas, descripción de los procedimientos de pruebas, resultados esperados de la prueba y resultados actuales de la prueba (ATE_FUN.1.1C)
	Los planes de prueba identifican las funciones de seguridad para ser probadas y describe las metas de las pruebas a desarrollar (ATE_FUN.1.2C)
	Las descripciones del procedimiento de prueba identifican las pruebas a desarrollarse y describe los escenarios para probar cada función de seguridad. Estos escenarios incluyen cualquier orden dependiendo de los resultados de otras pruebas (ATE_FUN.1.3C)
	Los resultados de las pruebas esperadas muestran las salidas anticipadas de una ejecución exitosa de las pruebas (ATE_FUN.1.4C)
	Los resultados de las pruebas de la ejecución del desarrollador demuestran que cada función de seguridad probada se comportó como se especificó (ATE_FUN.1.5C)
	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia (ATE_FUN.1.1E)
	El desarrollador provee el TOE para pruebas (ATE_IND.2.1D)
	El TOE se adecua para pruebas (ATE_IND.2.1C)
	El desarrollador provee un conjunto equivalente de recursos para esos que fueron usados en la prueba funcional del desarrollador de la TSF (ATE_IND.2.2C)
	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia (ATE_IND.2.1E)
	El evaluador prueba un subconjunto de la TSF apropiadamente para confirmar que el TOE funciona como se especificó (ATE_IND.2.2E)
	El evaluador ejecuta un ejemplo de pruebas en la documentación de pruebas para verificar los resultados de pruebas del desarrollador (ATE_IND.2.3E)

Tabla 5. Clase Pruebas - Preguntas para EAL1 y EAL2

EAL	Pregunta
EAL2	El desarrollador realiza un fuerte análisis de función de seguridad del TOE para cada mecanismo identificado en el ST como una fuerza que demanda función de seguridad del TOE (AVA_SOF.1.1D)
	Para cada uno de los mecanismos con una dotación de función de seguridad del TOE demanda la fuerza del análisis de función de seguridad del TOE que cumple o supera el nivel de fortaleza mínimo definido en el PP / ST (AVA_SOF.1.1C)
	Para cada uno de los mecanismos con una fortaleza específica de función de seguridad del TOE reclama la fortaleza del análisis de función de seguridad del TOE muestra que reúne o excede la fortaleza específica de funciones métricas definidas en el PP/ST (AVA_SOF.1.2C)
	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia (AVA_SOF.1.1E)
	El evaluador confirma que las solicitudes estrictas son correctos (AVA_SOF.1.2E)
	El desarrollador lleva a cabo y documenta un análisis de lo que se puede entregar del TOE buscando la manera evidente en la cual un usuario puede violar la TSP (AVA_VLA.1.1D)
	El desarrollador documenta la disposición de las vulnerabilidades evidentes (AVA_VLA.1.2D)
	La documentación presenta que para todas las vulnerabilidades identificadas, que la vulnerabilidad no puede ser explotada en el medio ambiente para el TOE (AVA_VLA.1.1C)
	El evaluador confirma que la información suministrada reúne todos los requisitos para contenido y presentación de evidencia (AVA_VLA.1.1E)
	El evaluador realiza pruebas de penetración, sobre la base del análisis de vulnerabilidad de los desarrolladores, para garantizar las vulnerabilidades evidentes que se han abordado (AVA_VLA.1.2E)

Tabla 6. Clase Evaluación de la Vulnerabilidad - Preguntas para EAL1 y EAL2

Cada pregunta se *califica* con 1 (si la respuesta es Verdadero) o 0 (en caso contrario). El nivel de riesgo de cada clase o total se calcula usando la siguiente fórmula:

100 - (puntaje obtenido x 100 / cantidad de ítems).

El resultado es equivalente al porcentaje de ítems no cubiertos –en la clase o en total según corresponda– y se usa para calificar el nivel de riesgo EAL, así: Muy alto (80 a 100%); Alto (60 a 80%); medio (40-60%); bajo (20-40%); y muy bajo (0 a 20%)

Cada pregunta se *califica* con 1 (si la respuesta es Verdadero) o 0 (en caso contrario). El nivel de riesgo de cada clase o total se calcula usando la siguiente fórmula:

100 - (puntaje obtenido x 100 / cantidad de ítems).

El resultado es equivalente al porcentaje de ítems no cubiertos –en la clase o en total según corresponda– y se usa para calificar el nivel de riesgo EAL, así: Muy alto (80 a 100%); Alto (60 a 80%); medio (40-60%); bajo (20-40%); y muy bajo (0 a 20%)

2.2. Evaluación en seguridad informática de productos de software de acuerdo con la ISO/IEC 15408 Common Criteria

Se propone un modelo que permita a los desarrolladores de software realizar la evaluación de sus productos, conceptualizados en un TOE (Target of evaluation) en seguridad informática, de acuerdo a la norma ISO/IEC 15408-3 Common Criteria en sus dos primeros niveles de evaluación (EAL1 y EAL2), que es permita identificar sus debilidades y formular las respectivas recomendaciones de mejora. El modelo (Ver Figura 3), incluye los siguientes componentes.

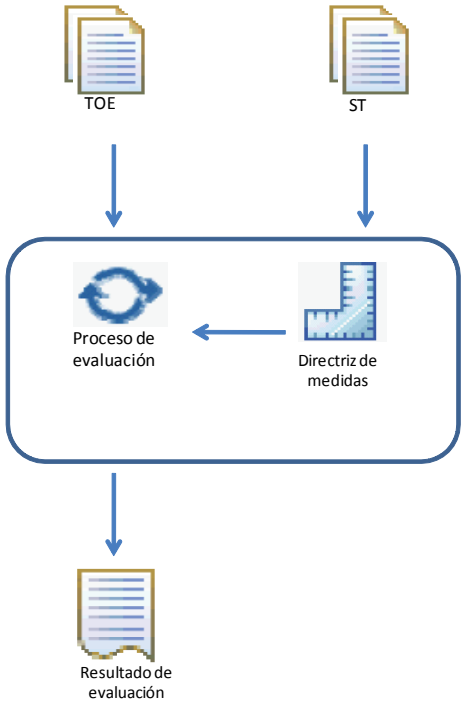


Figura 3. Modelo de ejecución de pruebas

» **ST** (Security Target). Objetivo de Seguridad. Documento oficial publicado en el Common Criteria, que describe las características de un TOE especifico

(Sistema de información, base de datos, sistema operativo o hardware) ideal dividido en: Límites Físicos (descripción del hardware donde se implementará el TOE); Limites Lógicos (descripción del software, que implementará el TOE, basado en sus funciones); entorno de seguridad del TOE (donde se identifican las hipótesis del entorno físico, características de los usuarios autorizados, las hipótesis del entorno lógico y las amenazas dirigidas al TOE y al ambiente operacional; Objetivos de seguridad (se especifican los objetivos que cumplirá el TOE en seguridad relacionados a autenticación y gestión de privilegios); y Requerimientos de seguridad (funciones y niveles de garantía de seguridad que cumple el TOE).

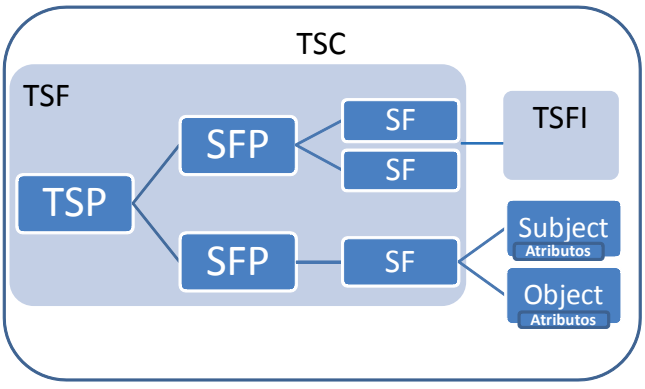
- **TOE** (Objetivo de evaluación). Componente TIC seleccionado para evaluar su seguridad bajo la norma ISO/IEC 15408 Common Criteria ST, dividido en límites físicos, lógicos, entorno de seguridad del TOE, objetivos de seguridad y requerimientos de seguridad.
- **Directriz de medidas**. De acuerdo a la importancia que se quiera dar a los ítems del ST, se establece una directriz de evaluación con un peso específico para cada ítem que permita generar un valor de calificación al aplicarse.
- **Proceso de evaluación**. Describe el conjunto de actividades para comparar el TOE con el ST, el cual aplica una directriz de medidas de acuerdo a lo similar que estos dos sean en sus especificaciones de entorno de seguridad, objetivos de seguridad, requerimientos de seguridad y niveles de seguridad.
- **Resultado de evaluación**. De acuerdo a los ítems del ST y la directriz de medidas, se presentarán un resultado de evaluación cuantitativo que permita establecer el nivel de seguridad del TOE a evaluar.

El modelo incluye dos roles. RTOE, responsable del TOE al que se le aplicará el modelo; y ETOE, responsable de la evaluación del TOE de acuerdo a las directrices determinadas. El primero debe conocer tanto el TOE que se va a evaluar, como la norma ISO/IEC 15408 Common Criteria, y tener la capacidad para implementar las mejoras que genere la aplicación del modelo de evaluación al TOE; el segundo debe conocer la norma citada y tener la capacidad de análisis necesaria para generar una evaluación objetiva del TOE

El flujo de actividades que incluye el modelo se describe a continuación, en su orden de ejecución. En todos los casos, en corchetes se incluye la información del componente al que pertenece y su responsable.

1. Seleccionar el Security Target (ST) [ST/RTOE]

Del repositorio de ST y Protection Profile (PP) que incluye el sitio oficial del Common Criteria se toma el más apropiado para la evaluación del software TOE. Para este tipo es necesario escoger en la sección *Other Devices and Systems ST* referentes a Sistemas de Información. Este modelo de evaluación se basará en el ST *SecureInfo Risk Management System Version 3.2.06.12 Security Target*



TSC: Scope of Control del TOE; TSP: TOE Security Policy; SFP: Security Function Policies; SF: Security Function; TSF: TOE Security Functions; TSFI: TSF Interface.

Figura 4. Distribución del TOE según sus componentes

2. Identificar características técnicas generales del TOE [TOE/RTOE]

El TOE se identifica con base en los componentes que muestra la Figura 4, que además presenta la relación entre ellos. En la figura, subjects se refiere a las entidades activas como procesos o usuarios que están sujetos a las políticas de seguridad del TSP; objects, a los objetivos de seguridad que se pueden realizar con los subjects; y attributes, a los atributos de seguridad necesarios para la definición de las políticas de seguridad del TOE. La distribución del TOE de acuerdo a sus componentes es la que se muestra en la Figura 4.

3. Especificar Límites Físicos [TOE/RTOE]

Los componentes en el hardware que soportará el TOE y la forma en que se conectarán (Id. LF1).

4. Especificar Límites Lógicos [TOE/RTOE]

Se definen las funciones de seguridad implementadas por el software que compone el TOE, las cuales son:

- Identificación y autenticación (Id. LL2). Se requiere la identificación y autenticación de los usuarios antes de acceder al TOE. No se debe iniciar ninguna modificación y/o eliminación sin previa identificación y autenticación. Cada usuario tiene asociado perfiles de seguridad con su cuenta que define las funcionalidades.
- Control de acceso (LL3). El TOE usa controles de acceso según las políticas establecidas por el área de TI.

5. Especificar entorno de seguridad [TOE/RTOE]

Se definen tres ítems en el TOE:

- Hipótesis del entorno físico (Id. EST1). Describe las características que previenen

el acceso físico no autorizado. Los recursos de procesamiento deben contar con entornos seguros con controles preventivos de accesos físicos no autorizados.

» Hipótesis del entorno de las TI (Id. EST2).Describe las características de operación del TOE, teniendo en cuenta: la conexión controlada de sistemas externos al TOE que interactúan con él, la protección de su hardware y software ante accesos no autorizados y la ejecución controlada de sus diferentes aplicaciones.

» Amenazas (Id. EST3). Describe las amenazas relacionadas con el TOE y el ambiente de TI. Las amenazas pueden ser: de *Acceso al TOE*, donde un usuario puede tener permisos por error de un usuario, por acción de un sistema o por un ataque sofisticado; y de *Acceso al ambiente operacional*, donde gane privilegios para realizar modificaciones no autorizadas.

6. Identificar objetivos de seguridad del TOE [TOE/RTOE]

Se especifican los objetivos de seguridad del TOE. Deben estar dirigidos a controlar el acceso de cualquier usuario autorizado y su gestión de privilegios a los recursos. (Responsable, RTOE). Su identificación es OS1.

7. Identificar funciones de seguridad [TOE/RTOE]

Se aplican las funciones de seguridad de referencia al TOE de acuerdo al ST escogido (ver Tabla 7).

Clase	Función de seguridad (Identificación)
FDP_ACC.1 Política control de acceso a un subconjunto	Asegurar la política de control de acceso a subconjuntos de usuarios, objetivos y operaciones específicas (Id. FS1)
FDP_ACF.1 Perfiles de seguridad basados en los controles de acceso	Controlar la seguridad del acceso basado en los atributos jerárquicos (Id. FS2)
	Aplicar el control de acceso de las políticas de las funciones de seguridad basándose en Permisos y/o dominios (Id. FS3)
	Aplicar reglas para determinar si una operación entre sujetos y objetos controlados está permitida (Id. FS4)
FIA_SOS.1 Verificación de datos de alta confidencialidad	Proporcionar un mecanismo para verificar el cumplimiento de las políticas y limitaciones de contraseña definidas por los atributos de: longitud mínima (8 caracteres) e inclusión de al menos un carácter alfabético, un carácter numérico y un carácter especial; no se deben reutilizar por el usuario; no debe indicar que la contraseña elegida está siendo usada por otro; debe prohibir contraseñas nulas durante la operación normal (Id. FS5)

Tabla 7. Descripción de las Funciones de Seguridad

Clase	Función de seguridad (Identificación)
FIA_UAU.2 Autenticación de usuarios antes de cualquier acción.	Exigir que cada usuario se autentique correctamente antes de permitir que cualquier otra función de seguridad del TOE realice acciones mediante el nombre de ese usuario (Id. FS6)
FIA_UAU.7 Protección de la información de autenticación.	Proporcionar solo información oculta para el usuario, mientras que la autenticación está en curso (Id. FS7)
FIA_UID.2 Identificación del usuario antes de cualquier acción.	Exigir que cada usuario se identifique antes de permitir que cualquier otra función de seguridad del TOE realice acciones en nombre de dicho usuario (Id. FS8)
FMT_MSA.1 Gestión de los perfiles de seguridad	Aplicar el control de acceso de la política de función de la seguridad para restringir la capacidad de cambio por defecto, consultar, modificar, eliminar y crear los atributos de seguridad: permisos del administrador del sistema del sistema de gestión y el administrador de dominio (Id. FS9)
FMT_MSA.3 Inicialización de atributos estáticos	Aplicar el control de acceso a la configuración del sistema, para hacer cumplir la SFP (Id. FS10)
	Permitir que el administrador del sistema de gestión y el administrador del dominio especifique valores iniciales para anular los valores por defecto cuando un objeto o la información es creada (Id. FS11)
FMT_MTD.1 Gestión de los datos de las funciones de seguridad del TOE	Restringir la capacidad de crear, consultar, modificar y eliminar los siguientes datos del TSF: grupo del sistema de gestión; permisos para grupos del sistema de gestión; cuenta de cliente de un grupo del sistema de gestión; y permisos para una cuenta de cliente del sistema de gestión (Id. FS12)
	Restringir la capacidad de crear, modificar y eliminar en ese dominio específico los siguientes datos: grupo del sistema de gestión; permisos para grupos del sistema de gestión; y cuenta de cliente de un grupo del sistema de gestión (Id. FS13)
FMT_SMF.1 Especificación de funciones de gestión	Ser capaz de realizar las siguientes funciones de gestión de seguridad: gestión de grupos del sistema de gestión; gestión de los permisos para cada grupo del sistema de gestión; gestión de cuentas de clientes en los grupos del Sistema de gestión; y gestión de permisos para cada cuenta del sistema de gestión (Id. FS14)
FMT_SMR.1	Mantener las funciones del administrador autorizado del sistema de gestión, los administradores de dominio y los usuarios autorizados (Id. FS15)
	Ser capaz de asociar a los usuarios los perfiles (Id. FS16)

Tabla 7. Descripción de las Funciones de Seguridad (cont.)

8. Identificar niveles de seguridad [TOE/ETOE]

Se aplica la norma ISO/IEC 15408-3 (Common Criteria). Nivel EAL1 (Probado funcionalmente) que evalúa si las funcionalidades del TOE corresponden a su documentación y no requiere una identificación detallada de riesgos; y Nivel EAL2 (Probado estructuralmente) que evalúa la entrega de la documentación del diseño y los resultados de las pruebas del TOE. (Responsable ETOE). Para cada pregunta y componente de la evaluación se realizará una descripción de su cumplimiento. Cada componente cuenta con un Id propio (NEXX).

9. Identificar evaluación seguridad [Directriz de medidas /ETOE]

Con base en las actividades anteriores se fija una evaluación y se aplica al TOE seleccionado. Se recomienda la siguiente ponderación: un punto en cada caso para el cumplimiento de las disposiciones en cuanto a límites físicos, límites lógicos, objetivos de seguridad y funciones de seguridad. Cinco, tres y dos puntos, para el cumplimiento de las disposiciones (tres, dos y una, disposiciones, respectivamente) respecto del entorno de seguridad del TOE.

10. Aplicar evaluación de seguridad [Proceso de Evaluación /ETOE]

Se aplica la evaluación para cada Id., de los límites físicos y lógicos, entorno, objetivos y funciones de seguridad, y su resultado se lee de acuerdo con la Tabla 8.

Nivel de cumplimiento	RANGO	DESCRIPCIÓN DE CUMPLIMIENTO
Ideal	22-21	Las funciones de seguridad están definidas completamente, junto con los límites y entorno de seguridad.
Adecuado	20- 16	Hay funciones de seguridad definido en su mayoría definidas, junto con los límites y entorno de seguridad
Aceptable	15-11	Existen límites, entorno de seguridad y más de la mitad de funciones de seguridad
Regular	10 – 6	Existen límites, entorno de seguridad definidos y ciertas funciones
Critico	5 – 0	Las funciones de seguridad no están completamente definidas junto con el entorno

Tabla 8. Niveles de cumplimiento del TOE

El nivel de cumplimiento debe ser consistente con el nivel de seguridad (Ver sección). Si el nivel de cumplimiento de los parámetros del TOE es Ideal, el nivel de riesgo EAL debe ser Muy bajo. De la misma manera, si el nivel de cumplimiento es Crítico, el nivel de riesgo debe ser Muy alto.

11. Generar reporte [Reporte/ETOE]

Con base en el cumplimiento del TOE, se genera un reporte con el resultado en general y la evaluación de cada Id.

3. Resultados

Con base en la información que presenta la Figura 5 se puede afirmar que el nivel de riesgo es alto, y que por complemento, el nivel de seguridad es crítico para los sistemas de información del muestro realizado, lo que podría indicar que la seguridad no ha tenido la prioridad debida. Esta valoración, realizada con la herramienta descrita en la sección 2.1 sustenta con creces la necesidad de generar y difundir modelos como el propuesto en este trabajo.

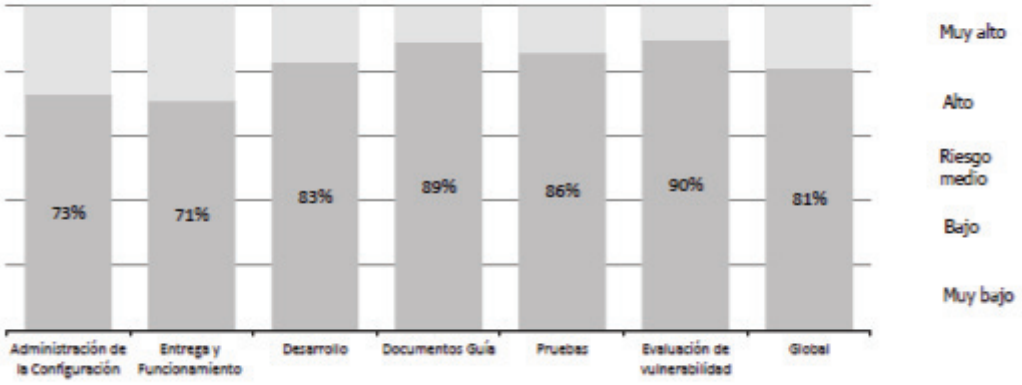


Figura 5. Resultados de la medición de nivel de riesgo EAL

Para aplicar el modelo descrito en la sección 2.5 se seleccionó el producto software *Sistema de Información para la Gestión de Activos* desarrollado por la empresa *Nexura International* (RTOE), un módulo de un ERP aplicado a una entidad pública. La empresa evaluadora (ETOE) fue *Password Consulting Services*, experta en servicios relacionados con seguridad informática. El ST (Secure Target) seleccionado fue el *SecureInfo Risk Management System Version 3.2.06.12 Security Target* (COACT, 2006). La aplicación arrojó como resultado: Cumplimiento adecuado, nivel de riesgo EAL bajo.

Como producto de la evaluación surgieron las siguientes recomendaciones:

Especificar Hipótesis del entorno físico y Amenazas con el fin de prever la protección del hardware y software del TOE ante accesos no autorizados, y la ejecución controlada en un ambiente especifico de las diferentes funciones del TOE.

Planear y ejecutar pruebas de seguridad y análisis de vulnerabilidades que permitan garantizar una revisión de la seguridad del TOE independiente al desarrollador y determinen sus debilidades, con el fin de preparar los ambientes de operación para evitar su explotación.

Con estos resultados se plantea la forma en que se aplica ejecución de pruebas de seguridad de productos software de acuerdo a la ISO/IEC 15408 Common Criteria.

Conclusiones y trabajo futuro

Las empresas clientes y proveedoras de Tecnologías de la Información deben ser más rigurosas con respecto a la documentación en el diseño del software, para mejorar el control y la gestión de la seguridad de sus componentes, además de presentar manuales detallados para la configuración y operación en ambientes seguros.

Para mejorar la seguridad del software a evaluar TOE la formalización en el lenguaje de expresión (Natural, Semi-Formal y Formal) es necesaria para lograr escalar los niveles de seguridad y acceder a posibilidades de certificación en el estándar ISO/IEC 15408 Common Criteria.

Ejecutar procesos de evaluación del software de la ISO/IEC 15408 permite complementar procesos en la compañías de implementación y certificación de ISO27001, que incluye requisitos de seguridad, seguridad en los procesos de desarrollo y gestión de las vulnerabilidades a los productos software que estén en el alcance del Sistema de Gestión de Seguridad de la Información (Instituto Colombiano de Normas Técnicas [ICONTEC], 2006, Anexo A.12).

Un centro de certificación en la ISO/IEC 15408 Common Criteria proyectaría a Colombia como un país gestor del mejoramiento de la seguridad de las TIC producidas en Latinoamérica y se presenta como una oportunidad de liderar procesos de competitividad, desarrollo e innovación en Tecnologías de la Información en la región.

El problema de los incidentes de seguridad en los sistemas de información de una entidad pública o privada no se soluciona completamente con la implementación y certificación de estándares, debido a que al final la decisión del usuario que opera es la que define en gran medida si ocurre o no un incidente. Sin embargo la adopción de estándares permite obstaculizar y rastrear para futuras investigaciones, esta clase de situaciones. S&T

Referencias bibliográficas

Aceituno, V (2006). ISM3 1.0. Information security management maturity model. Barcelona, España: ISECOM. http://hades.udg.es/~xavier/downloads/White_Papers/ISM3.es.1.0.pdf

Almanza, A. (2011). Seguridad informática en Colombia: tendencias 2010-2011. *Sistemas*, 119, 46-73. http://www.acis.org.co/fileadmin/Revista_119/Investigacion.pdf

APM Group (2007). Welcome to the official ITIL® Website. http://www.itil-officialsite.com/

Apuestas para crecer (2008, Octubre). *Revista Dinero*, 312, Recuperado de: http://www.dinero.com/caratula/edicion-impresa/articulo/apuestas-para-crecer/69337

Cano, J. (2004). Inseguridad informática: un concepto dual en seguridad informática. *Revista de Ingeniería* (19), 40-44. http://revistaing.uniandes.edu.co/pdf/Rev19-4.pdf

Cano, J., Samudio, E., Prandini, P., Corozo, E., & Almanza, A. (2011). *III Encuesta latinoamericana de seguridad de la información. ACIS, 2011* [Slides]. *Recuperado de* http://www.acis.org.co/fileadmin/Base_de_Conocimiento/XI_JornadaSeguridad/Presentacion_Jeimy_Cano_III_ELSI.pdf

COACT Inc. (2006). *Secureinfo risk management system Version 3.2.06.12 Security Target*. San Antonio, TX: SecureInfo. Recuperado de http://www.commoncriteriaportal.org/labs/

Common Criteria (s.f). *Licensed laboratories*. Recuperado de: http://www.commoncriteriaportal.org/labs/

Common Criteria. (2000). *Arrangement on the recognition of Common Criteria certificates in the field of information technology security*. Recuperado de http://www.commoncriteriaportal.org/files/operatingprocedures/cc-recarrange.pdf

Computer Security Institute [CSI]. (2011). *2010/2011 Computer crime and security survey*. New York, NY: CSI

Dirección General para el Impulso de la Administración Electrónica. (2011). Magerit versión 2. Recuperado de http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=184

European Network of Information Security Agency [ENISA] (2011). About Enisa. Recuperado de: http://www.enisa.europa.eu/publications/studies

Fernández, E., Moya, R., & Piattini, M. (2003). Seguridad de las tecnologías de la información: la construcción de la confianza para una sociedad conectada. Madrid, España: Aenor. ISBN 84-8143-367-5

Fraude en impuestos (2011, Noviembre 30). El Espectador.com. Recuperado de: http://www.elespectador.com/impreso/bogota/articulo-314297-fraude-impuestos

Herzog, P. (2010). OSSTMM 3 – The open source security testing methodology manual. Barcelona, España: ISECOM. http://www.isecom.org/mirror/OSSTMM.3.

Information Systems Audit and Control Association [ISACA]. (2011). *Cobit framework for IT governance and contro*l. Recuperado de http://www.isaca.org/knowledge-center/cobit/pages/overview.aspx

Instituto Colombiano de Normas Técnicas [ICONTEC] (2006). *Norma técnica NTC-ISO-IEC 27001:2005, Anexo A*. Bogotá, Colombia: ICONTEC.

International Organization for Standardization [ISO/IEC]. (2005a).

15408-1 Information Technology — Security techniques — Evaluation criteria for IT security part 1: Security functional requirements. Ginebra, Suiza: ISO

International Organization for Standardization [ISO/IEC]. (2005b). *15408-2 Information Technology — Security techniques — Evaluation criteria for IT security part 2: Security functional requirements*. Ginebra, Suiza: ISO

International Organization for Standardization [ISO/IEC]. (2005c). 15408-3 Information Technology — Security techniques — Evaluation criteria for IT security part 3: Security assurance requirements. Ginebra, Suiza: ISO

Internet Crime Complaint Center [IC^3]. (2010). *Internet crime report*. Richmond, VA: NWC^3. http://www.ic3.gov/media/annualreport/2010_IC3Report.pdf [Citado el 4 de Diciembre 2011

López, A., & Ruiz, J. (2005a). La serie 27000. Recuperado de http://www.iso27000.es/iso27000.html#section3b

López, A., & Ruiz, J. (2005b). *ISO27000*. Recuperado de: http://www.iso27000.es/iso27000.html

National Institute of Standards and Technology [NIST] (2011). Computer security division. Computer security resource center. Recuperado de http://csrc.nist.gov/

PoisAnon (2011). PoisAnon - Operation:RobinHood [Video]. Recuperado de http://www.youtube.com/watch?v=aymM8ONuQpg

SANS Institute (2011). *Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines*. Recuperado de http://www.sans.org/critical-security-controls/

Software Engineering Institute [SEI]. (2008). *Octave*. Recuperado de http://www.cert.org/octave/

SYMANTEC (2011). *Descripción general de la tecnología*. Recuperado de: http://www.symantec.com/es/es/about/profile/Technology.jsp

Zone-h.org (2010). Ataque a UNE. Recuperado de http://www.zone-h.org/mirror/id/10272455

Currículum vitae

José Alejandro Chamorro López, M.Sc.

Máster en Gestión Informática y Telecomunicaciones y Especialista en Redes y Comunicaciones de la Universidad Icesi, Colombia; Auditor ISO27001; Ingeniero en Electrónica y Telecomunicaciones, Universidad del Cauca, Colombia; Consultor en Seguridad de la Información en Password Consulting Services desde hace siete años en servicios de Ethical Hacking Análisis de Riesgos y Análisis Forense Informático, para más de 50 compañías en el sector público y privado.

Francisco Pino, Ph.D.

Doctor en Tecnologías Informáticas Avanzadas (Universidad Castilla-La Mancha, España), Especialista en Redes y Servicios Telemáticos e Ingeniero en Electrónica y Telecomunicaciones (Universidad del Cauca, Colombia). Integrante del Grupo de Investigación y Desarrollo en Ingeniería del Software y docente del Departamento de Sistemas de la Facultad de Ingeniería Electrónica y Telecomunicaciones de la Universidad del Cauca. Es miembro de los grupos de ejecución de los proyectos: Mejora de procesos para fomentar la competitividad de la pequeña y mediana industria del software de Iberoamérica, Mejora basada en evidencia de la capacidad en actividades de Software, Evolución de Software Factories mediante ingeniería del software empírica y Reunión de especialistas en verificación y validación de software, y miembro de la red Calidad del Producto y Proceso de Software.